Federal Maritime Commission Information Technology Strategic Plan FY 2018-2022

December 2018

Table of Contents

Message from the CIO

The Federal Maritime Commission (FMC or Commission) is pleased to issue its Information Technology Strategic Plan for Fiscal Years 2018-2022 (IT Strategic Plan or Plan). This updated IT Strategic Plan reflects our progress with prior fiscal years' (FY) IT initiatives, next steps, and alignment with the FMC's FY 2018-2022 Strategic Plan. It replaces the Commission's FY 2014-2018 Information Resources Management Plan and is the first FMC IT Strategic Plan developed since the enactment of the Federal Information Technology Acquisition Reform Act (FITARA) and related OMB guidance. This Plan incorporates IT priorities of the Commission as it continues to focus on moving from paper-based systems to electronic systems, strengthening our cybersecurity program, improving the quality of IT services and solutions, and administration of information technology at the FMC. The objectives and initiatives outlined in this Plan directly support the Commission's mission and strategic goals.

Digital transformation is enabling better IT-business alignment and transforming government. As with other Federal agencies, the FMC is undergoing a digital transformation, shifting how it interacts with and delivers services to the shipping industry. These changes continue to drive a focus upon shared service strategies, customer-centric operations, and securing data across platforms and devices.

This Plan is the result of the commitment and dedication of our FMC team. It represents a collaborative effort across the Commission to ensure that we realize the full benefits of IT as we look at opportunities to improve our capabilities to meet future needs.

Anthony Haywood
Chief Information Officer
Federal Maritime Commission

About the Federal Maritime Commission

History and Statutory Authority

First constituted over 100 years ago as the United States Shipping Board in the Shipping Act of 1916, the Federal Maritime Commission was authorized in its current form as an independent Executive Branch agency in 1961. The Commission's mission is to ensure a competitive and reliable international ocean transportation system that supports the U.S. economy and protects the public from unfair and deceptive practices.

The Commission will achieve its mission by ensuring that the fundamental dynamics of a free, open, and competitive ocean transportation market drive economic outcomes. The Commission is committed to administering the Shipping Act while employing a minimum of government intervention and regulatory costs, and by placing a greater reliance on the marketplace. Congress assigned these responsibilities to the FMC in the following laws now codified at 46 U.S.C. §§ 40101-44106:

- The Shipping Act of 1984, as amended by the Ocean Shipping Reform Act of 1998;
- The Foreign Shipping Practices Act of 1988;
- Section 19 of the Merchant Marine Act, 1920; and
- Sections 2 and 3 of Pub. L. No. 89-777, 80 Stat. 1350.

Mission and Strategies

The Commission is composed of five Commissioners appointed by the President with the advice and consent of the Senate. Commissioners serve five-year, staggered terms, and no more than three members of the Commission may belong to the same political party. The President designates one of the Commissioners to serve as Chairman. The Chairman is the chief executive and administrative officer of the agency.

The Commission carries out its regulatory responsibilities by conducting informal and formal investigations. It holds hearings, considers evidence, renders decisions, and issues appropriate orders and regulations. The Commission also adjudicates and mediates disputes involving regulated entities, the shipping public, and other affected individuals or interest groups.

As set forth in the Commission's current Strategic Plan, the FMC's mission is to ensure a competitive and reliable international ocean transportation supply system that supports the U.S. economy and protects the public from unfair and deceptive practices. The following strategic goals and objectives enable the FMC to accomplish that mission:

Strategic Goal 1: Maintain a competitive and reliable international ocean transportation supply system.

> **Objective 1.1:** Ensure that actions under filed agreements do not result in unreasonable increases in transportation costs and/or unreasonable decreases in transportation services.

Strategic Goal 2: Protect the public from unlawful, unfair, and deceptive ocean transportation practices.

> **Objective 2.1:** Identify and take action to end unlawful, unfair, and deceptive practices.

> **Objective 2.2:** Prevent public harm through licensing and financial responsibility requirements.

> **Objective 2.3:** Enhance public awareness of agency resources, remedies and regulatory requirements through education and outreach.

> **Objective 2.4:** Impartially and timely resolve international shipping disputes through alternative dispute resolution and adjudication.

IT Strategic Plan Overview

The Paperwork Reduction Act of 1995 (PRA), as amended, and the Office of Management and Budget (OMB) Circular A-130, *Management of Federal Information Resources*, require the Federal Maritime Commission to develop and annually revise a five-year plan for meeting its information technology needs. The Clinger-Cohen Act, or Information Technology Management Reform Act of 1996 (ITMRA), and the Federal Information Technology Acquisition Reform Act of 2014 (FITARA), require agencies to acquire IT in the most efficient and cost-effective manner.

The FMC's Office of Information Technology (OIT) provides IT management, technical, and administrative support to the Commission's program operations. Based on the above government-wide requirements, this IT Strategic Plan describes the OIT's vision and initiatives, and details its approach for carrying out those initiatives. The Plan provides a basis for addressing agency-wide IT needs, including individual bureau and office needs. The Plan is linked to its parent document, the agency's Strategic Plan covering FY 2018-2022, and has been integrated within the agency's policy and decision-making processes. This ensures the IT Strategic Plan aligns with the FMC's mission and strategic objectives.

Preparation of this Plan also has been coordinated with the requirements of the Commission's *Automated Information Security Program* (Commission Order 56) and *Information Security Incident Response Policy – Breach Notification Plan* (Managing Directive 2). These documents help ensure that access to information, resources, and services are limited to authorized personnel, and that the confidentiality, integrity, and availability of information resources are

not diminished due to misuse of agency-owned/issued technology. This IT Strategic Plan provides the approach that OIT will take to address the challenges of delivering IT services in an environment of rapid digital change and evolving cybersecurity threats, while keeping abreast of continuous advancements in technologies.

OIT has identified several overarching challenges which are addressed by this 5-year Plan, including:

- consolidating and upgrading legacy applications and infrastructure with newer technologies,
- implementing automation to streamline workflow processes and improve efficiency, and
- integrating security standards and frameworks to protect from cybersecurity risks, agency-owned/issued assets and commercially sensitive data collected from the shipping public.

To address these challenges, OIT has identified four IT strategic goals targeting quality, efficiency, cybersecurity, and compliance. Each goal is broken down into specific action-oriented objectives supported by key initiatives specifically designed to support each goal.

IT Strategic Goal 1 – Manage and deliver quality IT systems and services critical for the FMC to fulfill its mission and support related administrative, business, and operational functions.

OIT is committed to delivering systems and services in support of the FMC's mission to improve functionality and reduce operational costs. This Plan requires the FMC to modernize its legacy line-of-business applications and to replace paper-based document management with modern technologies and customer-centric services. In addition, OIT will enhance administrative and operations policies, tools, and systems needed to maintain and support the agency's business. OIT will also perform capacity planning to ensure that the IT infrastructure is able to meet anticipated business growth as well as administrative and operational functions.

Objective 1.1: Improve utilization of technology

Key Initiatives:

1.1.1   FMC Electronic Records Modernization Initiative

This initiative will establish an agency-wide policy framework and enterprise architecture for electronic records management and design. Improving operational efficiency and reducing costs by replacing paper-based records processes with automated workflow and document management solutions will be a major outcome of this initiative. The Commission's enterprise architecture for electronic records management will ensure full compliance with the National Archives Records Administration (NARA) Managing Government Records Directive M-12-18.

Directive M-12-18 requires that agencies manage permanent records in an electronic format by December 31, 2019. This initiative will improve the FMC's records storage and management services for Commission-owned paper and electronic records in accordance with OMB Circular A-130, which requires that agencies incorporate records management requirements into their cloud-based storage and service solutions.

Target Completion Date: 4th Quarter FY 2019

Objective 1.2: Modernize Legacy Applications

Key initiatives:

1.2.1 Service Contract Filing System and Database Upgrade

This initiative will upgrade the current Service Contract Filing System (SERVCON) application and database environment. SERVCON is a web-facing filing system for ocean common carrier service contracts and non-vessel-operating common carrier (NVOCC) service arrangements. The FMC uses SERVCON to review service contracts and agreements to ensure that the service contracts and NVOCC service arrangements comport with the requirements of the Shipping Act.

Target Completion Date: 3rd Quarter FY 2018

1.2.2 Design, Implement, and Deploy a new Ocean Transportation Intermediary (OTI) License, Registration, and Application Processing System

The FMC currently supports a public-facing online OTI license application process. However, the external users often require assistance from FMC staff due to browser incompatibility and system intuition issues. Additionally, license application data received requires manual entry, review, and manipulation by the FMC staff due to the existence of four discrete databases used for license application processing. The new system will eliminate the need and constraints of multiple databases; reduce the burden to external and internal users; increase responsiveness of the FMC staff; and provide new technology for licensing registration, and bond surety transactions. The goal is to automate and integrate the entire process, cutting redundancy, improving efficiency, and decreasing processing time for both staff and external stakeholders.

> **Regulated Persons Index (RPI) Enterprise Data Store and Reporting** – The RPI is a Commission database containing OTI license, registration, and surety bond information. This initiative will automate the current process of manually entering data from a Form FMC-18 OTI application into the RPI system and expand the scope of the RPI to allow the following modules to directly communicate and populate new and updated status information to the RPI database:
>
> - Form FMC-18 (OTI Applications and Back Office Processing),
>
> - Form FMC-48 OTI Surety Bonds (E-Bond),

- Form FMC-1 Tariff Locator,

- Form FMC-18 License Renewal and Self-Service, and

- Form FMC-65 Foreign-Based OTI Registration, Renewal, and Self-Service.

The RPI will be the single database for use by licensees, applicants, registrants, OTI surety companies, and tariff publishers resulting in the consolidation of four currently discrete databases into one, and increased efficiencies for internal and external users.

OTI Application and Back Office Module- This project will develop a new OTI licensing module to provide a fully integrated and user-friendly online interface that will streamline internal FMC licensing processes, pre-populate data for external users, and include data fact checking functions that will automatically "flag" issues with data entered into the system by the OTI license applicant. This module will also integrate internal and external OTI-related services and business processes to support license requirements and reduce processing time.

Electronic Bond (E-Bond) Module – This initiative will develop a web-facing module to enable online filing of OTI surety bonds (current Form FMC-48) and reporting of claims by surety companies. This function is currently completely manual.

Automated Tariff Registration Module – This initiative will fully automate the FMC's Automated Tariff Registration (current Form FMC-1) module, business process, and FMC staff review process. The Automated Tariff Registration module facilitates the registration of tariff publication locations by NVOCCs, as well as ocean common carriers, conferences, and marine terminal operators (MTOs).

OTI License Renewal and Self-Service Module – This project will develop a new OTI licensing case management module to provide a fully integrated and user-friendly online interface to support OTI license renewal activities. This module will integrate internal and external OTI-related services and business processes to support license renewals required of U.S.-based OTIs every three years. Currently the license renewal process is automated as part of the online Form FMC-18, however day-to-day license and registration updates are primarily manual, which creates inefficiencies externally and internally.

Foreign-based OTI Registration, Renewal, and Self-Service Module This project will develop a new registration, renewal, and self-service module for foreign NVOCCs (currently processed under Form FMC-65) to provide a fully integrated online, paperless interface supporting OTI electronic registration, renewal and internal processing activities. The application will expand the use of the existing renewal system to allow registrants to update, change/review information submitted during the renewal period. Currently the triennial renewal procedure has been automated

but most of the other processes envisioned for this module remain manual, which creates inefficiencies externally and internally.

Target Completion Date: 2nd Quarter FY 2020

1.2.3 Deploy new Electronic Reading Room and Docket Filing System

This initiative will replace that portion of the FMC's current online electronic reading room containing the activity logs of the public filings and documents issued by the Commission or FMC Administrative Law Judges in FMC formal and informal adjudicatory proceedings, rulemakings, petitions, fact findings, and investigations, with a new web-based information system. The new electronic reading room system will provide public filers the ability to file documents directly into the system and automate the posting of filed documents to the appropriate docket/proceeding log for public viewing through the FMC's public website. The new system will streamline internal processes by eliminating current additional steps in the posting process and facilitate internal circulation and review of filed documents.

Target Completion Date: 2nd Quarter FY 2021

1.2.4 Deploy Updated Port Import Export Reporting Service (PIERS) Interactive Application

The Bureau of Trade Analysis (BTA) relies extensively upon a commercial trade data reporting service (PIERS) to provide aggregate trade, commodity, and carrier market share information derived from foreign waterborne data collected by the U.S. Customs and Border Protection. This interactive application allows BTA to download, store, and run a host of customized trade reports critical to its review of carrier and MTO agreements under the provisions of the Shipping Act. The new version of this application will upgrade PIERS Interactive to current technology to improve performance.

Target Completion Date: 4th Quarter FY 2021 or later

1.2.5 Design and Deploy new Passenger Vessel Operator Filing System

Deploy an automated processing and reporting application for the filing of passenger vessel operator (PVO) financial responsibility certificates, and to track and analyze unearned passenger revenue (UPR) as reported by PVOs under 46 CFR Part 540.

Target Completion Date: 4th Quarter FY 2022 or later

1.2.6 IT Operations & Maintenance (O&M) Support for Applications and Systems Maintenance and Upgrades

After an application/system is launched and released into the FMC's production environment, applications and systems are tested and maintained to ensure each application/system is fully functional and performing optimally until the platform reaches its end of life. During this operation and maintenance phase, OIT will provide

application engineering, troubleshooting, operations maintenance, and administration services in accordance with software development life cycle best practices.

Target Completion Date: Ongoing

Upgrades and development of new applications included in the FMC's IT Strategic Plan and scheduled through FY 2022 are shown in the table below:

IT Systems to be Updated	FY 2018	FY 2019	FY 2020	FY 2021	FY 2022	Notes
SERVCON Update	Deployed	Deployed	Deployed	Deployed	Deployed	Update of service contract filing system completed in FY 2018
Electronic Records Initiative	$100,000	$100,000	Deployed	Deployed	Deployed	Projected completion in FY 2019
OTI License, Registration, and Application Processing System						
Regulated Persons Index (RPI) Data-Store integration	$1,097,000 includes related applications	$1,123,000 includes related applications	$600,000 includes related applications	Deployed	Deployed	Central Database serves as backbone to integrated system. Internal workflow processes will integrate with public-facing front end and 5 modules listed below.
OTI Application/ Back Office Module	In development	In development	Testing and deployment	Deployed	Deployed	Internal workflow processes will integrate with public facing front-end and related modules.
Electronic Bond (E-Bond) Module	In development	In development	Testing and deployment	Deployed	Deployed	E-filing system for OTI sureties will be developed in conjunction with related modules.
Tariff Registration Module	In development	In development	Testing and deployment	Deployed	Deployed	Stand-alone OTI tariff locator (Form FMC-1) will integrate with related modules.
OTI License Renewal and Self-Service Module	In development	In development	Testing and deployment	Deployed	Deployed	Developed in production system, will migrate to new integrated OTI system when deployed.
Foreign OTI Registration, Renewal, and Self-Service Module	In development	In development	Testing and deployment	Deployed	Deployed	Developed in production system, will migrate to new integrated OTI system when deployed, replacing Form FMC-65.
Electronic reading room and dockets filing system	Future	Future	$236,825	$400,000	Deployed	Development begins FY 2020 following deployment of OTI License, Registration, and Application Processing System.
PIERS Interactive	Future	Future	Future	$436,825	Deployed	Deploy in 2021 or later
Passenger Vessel Operator Filing System	Future	Future	Future	Future	$400,000	Deploy in FY 2022 or later
Operations & Maintenance (incl. app upgrades)	n/a	n/a	n/a	n/a	$436,825	Applications maintenance; future application updates to be prioritized by ITAB
Total IT consulting services (in $ per current fiscal year)	$1,197,000	$1,223,000	$836,825	$836,825	$836,825	Subsequent OIT deployments contingent on funding

IT Strategic Goal 2 – Maintain IT policies, procedures, and practices that support efficient and effective FMC business, administrative, and mission processes.

With the implementation of new information systems, governmental mandates and regulations, the FMC's supported IT infrastructure continues to grow. This Plan supports the improvement of FMC mission-critical functions by consolidating systems and eliminating redundant and outdated applications and services to streamline FMC processes, while realizing long-term cost savings.

Objective 2.1: Continue to update policies and procedures for IT management to ensure systems and services are managed in an efficient, effective, and economical manner

Key Initiatives:

2.1.1 Develop standardized framework for application development

The aim of this initiative is to deliver a common development approach by which OIT will effectively deliver software and information system architectures, requirements, and designs across the agency.

Target Completion Date: 1st Quarter FY 2019

2.1.2 Continue to improve the acquisition and fiscal management accountability for the IT capital planning, budget formulation, execution and tracking processes through early and continuing engagement with the Information Technology Advisory Board (ITAB).

The ITAB advises the Commission on IT issues applicable to the agency. The ITAB is responsible for reviewing IT planning and the budget appropriate to support information technology including application development, business continuity and disaster recovery, information security, data management, and user support, as well as network and telecommunications systems maintenance.

Target Completion Date: 3rd Quarter FY 2018

Objective 2.2: Develop and retain a highly skilled technical team

Key Initiatives:

2.2.1 Develop a career growth program for progression of OIT staff to the next level technical position.

Target Completion Date: Review annually

2.2.2 Develop talent retention and succession planning strategies for OIT.

Target Completion Date: Review annually

2.2.2 Review IT Position Descriptions (PD) for updates, as applicable.

Target Completion Date: Review annually

IT Strategic Goal 3 – Expand on current progress to strengthen cybersecurity of FMC's networks and systems.

The FMC Cybersecurity Program provides cybersecurity capabilities and risk management methodologies to protect sensitive data and information systems in support of the Commission's mission and ensures the protection of privacy, confidentiality, integrity and availability of information. OIT directs the activities and the functions of the FMC's information security program, and develops and maintains information security policies, rules, and control techniques to address the responsibilities assigned to the Commission under the Federal Information Security Management Act of 2002 (FISMA) and other governing statutes, regulations, and policies.

This Plan outlines initiatives for continuous improvement of the Commission's cybersecurity policies and standards, audit review coordination, security awareness training program, and related security requirements of the FMC's information and information systems development.

Objective 3.1: Deploy cybersecurity tools and technologies to protect agency-owned/issued assets, and personally identifiable information (PII) contained in FMC-maintained IT systems.

Key Initiatives:

3.1.1 Develop and Manage a Comprehensive Cybersecurity Program

Enhance and strengthen the FMC Cybersecurity Programs to conduct effective incident response, insider threat detection, situational awareness, governmental regulation and mandate compliance, and to reduce the overall security risk to Commission information and IT infrastructure.

Target Completion Date: 2nd Quarter FY 2022

3.1.2 Implement Continuous Diagnostic and Mitigation (CDM) capabilities.

This project will continue to fortify the Commission's cybersecurity systems and network by implementing Phase 1 of the Department of Homeland Security (DHS) CDM program capabilities, tools, and services. The CDM Program covers 15 continuous diagnostic capabilities and rolls these out in three phases. The first phase of CDM focuses on endpoint integrity: management of hardware and software assets, configuration management, and vulnerability management. (DHS is further defining phases 2 and 3 to include identity and infrastructure management.)

Target Completion Date: 2nd Quarter FY 2022

Budgetary Estimates					
Requirement	FY2018	FY2019	FY2020	FY2021	FY2022
Continuous Diagnostic and Mitigation (CDM) Program tools and services rollout		$18,765	$20,640	$22,705	$24,976

3.1.3 Implement an Information Systems Security Line of Business (ISSLoB) program.

Where appropriate to support the Commission information systems security needs, the FMC will implement DHS's ISSLoB services, including security and awareness training, situation awareness, and incident response shared products and services, including access to blanket purchase agreements, where appropriate.

Target Completion Date: 4th Quarter FY 2022

3.1.4 Continue implementation of the Federal Information Technology Acquisition Reform Act (FITARA) and related IT management practices.

The Commission will continue to implement the requirements and IT management controls of FITARA as outlined in Office of Management and Budget Memorandum M-1-14.

Target Completion Date: 2nd Quarter FY 2021

IT Strategic Goal 4 – Ensure reliability and accuracy of federal information technology as required by statutes, government-wide requirements, directives, or guidance.

Objective 4.1: Update or develop policies and programs consistent with current government-wide requirements, OMB directives, and reporting requirements designed to protect agency IT assets and PII.

Key Initiatives:

4.1.1 Enhance FISMA-related security program

Review and update policies and rules for the Commission's Certification & Accreditation program, Insider Threat Detection program, support Privacy Act compliance, and ensure compliance with and enforcement of DHS cybersecurity risk management mandates.

Target Completion Date: 2nd Quarter FY 2020

4.1.2 Develop and manage Privacy Continuous Monitoring Program

In implementing agency's Cybersecurity Program, it is essential to take a coordinated approach to identifying and managing security and privacy risk within the FMC. This project will develop and manage a privacy continuous monitoring (PCM) program in accordance with the approach outlined in OMB Circular A-130, FISMA, NIST Risk Management Framework, NIST Special Publication (SP) 800-37 and other federal

guidance, to ensure risk are effectively monitored and controls are commensurate with the federal security and privacy directives.

Target Completion Date: 2th Quarter FY 2019

4.1.3   Develop Service Level Agreements (SLAs) with metrics tracking to ensure accountability of services.

Implement continuous service improvement processes (i.e., Service Level Agreements and Operation Level Agreements (OLAs)) to ensure that customers are provided services in a timely manner. Leverage IT service management to implement Information Technology Infrastructure Library governance models and methodologies.

Target Completion Date: 1st Quarter FY 2019

4.1.4   Provide comprehensive oversight and guidance by IT personnel responsible for managing IT contracts and acquisitions.

Ensure all contract language that affects the management of data is up to date and in compliance with all provisions stated in NIST 800-53, Rev.4, as revised, for the SA-4 acquisition process control. The FMC's Information Systems Security Officer (ISSO) shall provide the appropriate language to OMS who will ensure that this language is included in every data management contract before award is made.

Target Completion Date: 3rd Quarter FY 2018

Current FMC IT Infrastructure

Agency-wide: FMC headquarters and regional offices have desktop and laptop computers linked to the Commission's local area network and wide area network (LAN/WAN), which interconnects computers and network devices for the agency. The FMC uses Microsoft Active Directory Domain Services (AD DS), Microsoft Server 2012 R2, Azure Active Directory (Azure AD), Windows 8, and Windows 10.

Local Area Network: Software applications on the network include Microsoft Office 2013/2016, Microsoft Office 365, Adobe Acrobat 10/DC, WordPerfect Office X5, Microsoft Internet Explorer 11, Google Chrome, Safari Firefox, Symantec Endpoint Protection, Cylance, Varonis, Microsoft Project Professional 2016, Microsoft Visio Professional 2016, BMC Track-IT, and Dell Desktop Authority Management Suite.

Specialized programs and systems: Specialized programs and systems which support bureau and office operations include: Pay.gov, Laserfiche, Westlaw LexisNexis, BPD Bureau of the Fiscal Service ARC PRISM platform, CBP Automated Commercial Environment (CBP ACE) and SERVCON in Azure.

Network and Infrastructure: The FMC's network runs on a 10-gigabit backbone with 1-gigabit connections to agency desktops and laptops. Internet services and Managed Trusted Internet

Protocol Services (MTIPS) are provided through CenturyLink MTIPS FMS's headquarters building and six regional Area Representative offices.

Federal Shared Services: The agency uses inter-agency shared services provided by U.S. Customs and Border Protection, the Department of the Treasury's Federal Financial Management System and the Bureau of the Fiscal Service, and the U.S. Dept. of Agriculture's National Finance Center.

The FMC has implemented federal cloud computing strategy in updating and modernizing the agency's technology infrastructure. Currently, there are four applications that have been migrated from on-premise servers to SharePoint Online and one application that was built completely on Microsoft's Azure cloud computing platform.

IT Modernization Challenges Facing the FMC

This Plan outlines the core objectives for modernizing the Commission's IT program, projects for legacy IT operations and maintenance investments, and IT that must be updated or replaced under existing federal mandates and guidance.

As with many federal agencies, attempts to modernize the FMC's systems have been hindered by a lack of available funding. Until the plans to modernize or replace these IT investments are finalized and fully executed, the Commission runs the risk of maintaining systems that have outlived their effectiveness.

Cybersecurity

This plan outlines the Commission's vision and key initiatives to build a modern and more secure architecture for its IT systems. Working in conjunction with federal IT enterprise partnerships on cybersecurity initiatives to ensure successful implementation of OMB, DHS, and other federal mandates, efforts to improve the Commission's security posture are ongoing and cover a significant part of the FMC's modernization plan. These cybersecurity efforts align with ongoing work to improve our citizen-facing services and improve security across the agency.

Government-wide Initiatives and OMB Directives

The Commission, like other small federal agencies, faces challenges in meeting the multitude of required IT-related government-wide initiatives, OMB directives, and reporting requirements. Many of these requirements were crafted for much larger federal agencies and Departments, and are not readily scalable to smaller organizations, IT budget and IT staffing levels. These challenges will be addressed through diligent planning and conscientious use of appropriated funds.

IT Modernization Project Funding

The success of the Commission's IT modernization plan is ultimately linked to funding availability, and it is expected that the Commission's budget appropriation will remain flat or result in moderate growth. Key funding challenges include updating legacy systems as necessary, OMB-mandated FISMA compliance, annual life cycle management of IT components, implementation of the Federal IT Shared Services Strategy, and the federal government's cloud first policy.

With express support from OMB and Congress, the Commission prioritized improving its IT systems through a multiyear project, now underway, to greatly improve its efficiency, reliability and cybersecurity readiness. Should these investments be fully implemented, the Commission's internal business processes would be automated or enhanced, legal and economic research and analysis capabilities will be improved and expanded, and better public access to FMC information will be facilitated. These improvements remain key to controlling future FTEs and permitting the FMC options for reallocating existing personnel to critical program needs in the future, consistent with its 5-year plan responsive to OMB Memorandum on *Reforming the Federal Government and Reducing the Federal Workforce*.